Research Paper | Cybersecurity | E-ISSN No : 2454-9916 | Volume : 9 | Issue : 6 | June 2023

CONCERNS OF PRIVATE DATA BEING MISUSED BY ARTIFICIAL INTELLIGENCE

Kopal Dokania

Research Scholars Program, Harvard Student Agencies, In collaboration with Learn with Leaders

ABSTRACT

This research paper examined potential privacy concerns, examined how private data is being misused, and considered how artificial intelligence can potentially play a significant role in the same. Private data was investigated, along with its potential for misuse and how it has grown to be the century's largest corporate sector thanks to links to the concept of the Placebo Effect. The research consistently emphasized artificial intelligence, its function in the modern world, and its potential power. It then looks at how artificial intelligence can be employed as a tool to misuse people's personal information, and later discusses how artificial intelligence could be used to limit data exploitation. However, when private information is taken and sold, it could help people in a variety of ways, including tracking down criminals using algorithms, predicting epidemics and treating diseases, and improving services and goods by different companies that will give customers a better quality and luxurious feel, and so much more that could be improved and benefited from the private data of the public that gets collected and ultimately sold to major corporations.

KEYWORDS: Privacy, Artificial Intelligence, Algorithms,

INTRODUCTION

Private data is information that a person has about themselves that is not accessible to the general public. Passwords, bank information, transactions, etc. may all fall under this category. Any personal, personally identifiable, or financial information may also be referred to as private data. Private information must be protected because if it falls into the wrong hands, bad things may occur. For instance, a data breach at a government organization may expose sensitive information to adversary nations. Constantly, it is crucial to maintain one's data private as it prevents the information of a business from fraudulent activities, hacking, phishing, and identity theft. Any corporation that wants to operate efficiently must create a data protection plan to secure the security of its information. AI analytics is a subset of business intelligence that makes use of machine learning methods to unearth new patterns, correlations, and insights in data. In order for the software to learn automatically from patterns or features in the data, artificial intelligence (AI) combines massive amounts of data with quick, iterative processing and sophisticated algorithms. In order to manipulate data and analyze it, which will be extremely helpful for us in order to track down criminals using algorithms, predict epidemics and treat diseases, use businesses to improve their services and goods, and much more as well, artificial intelligence is able to combine large amounts of data sets and form patterns quickly. This research paper will mainly focus on an analysis of private data being misused by Artificial Intelligence indicating that when private information is taken and sold, it could have both, positive and negative, implications connecting to it.

What Is Privacy of Data & Its Worth

Data privacy refers to the ability of an individual to control the sharing of their personal information with others. Personal information may include one's name, address, phone number, or online and offline conduct. As the use of the internet has grown, so has the significance of data privacy. Websites, software, and social media platforms often need to collect and preserve personal data about users to deliver services. However, some platforms and applications may exceed users' expectations in terms of data collection and utilization, compromising their privacy. Additionally, some platforms may not provide adequate protection for the data they collect, which may result in data breaches.

Data protection regulations exist to safeguard the right to privacy, which is considered a fundamental human right. Businesses use data protection procedures to demonstrate to their clients and users that they can be trusted with their personal information. While some businesses may underestimate the value of public data, they will need to become more skilled in evaluating their assets in the future. Although there is no consistent method for determining the exact value of data, it is estimated to be worth hundreds of billions of dollars. With the creation of trillions of data points, the lack of verification becomes a problem. Big data and tailored marketing provide a high return on investment. However, the cost of vetting would eliminate a significant portion of the profit margin that drives enormous amounts of business earnings and sales for firms like Facebook and Google. Therefore, it is not uncommon for a 30-year-old single man without children to receive advertisements for baby products after purchasing a baby-themed item for his sister's new baby. Many internet users are familiar with this type of mistake.

However, Big Data and targeted marketing continue to expand and thrive in spite of these issues. In the USA alone, the data sector now generates $300 billion a year and employs 3 million people, while in the UK, publishers and content producers earn £10 billion a year from digital advertising. Businesses will evolve along with consumer internet usage as it grows and transforms from a useful tool to a necessary component of everyone's lives. Businesses will market and sell to us more and more on an individual basis rather than spending a fortune on large-scale, all-encompassing advertising projects.

In conclusion, data privacy is an essential aspect of online activity, and businesses must take adequate measures to safeguard their users' personal information. Data protection regulations are in place to protect individuals' fundamental right to privacy. Although data is valuable, the lack of verification may lead to problems in the future. Firms will need to become more skilled in evaluating their assets while balancing the need for vetting against profit margins.

How Private Data Is Misused

Eric Schmidt is famous for saying, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" when he was the CEO of Google. The British government chose the catchphrase "If you've got nothing to hide, you've got nothing to fear" to advertise a widespread CCTV surveillance program using the same logic. These instances show how various privacy violations' negative effects on law-abiding persons are frequently disregarded, underappreciated, or even purposefully hidden. As a result, many people, including judges, find it difficult to explain why protecting personal information is crucial.

The role of data protection advocates has been under scrutiny with the labelling of such advocates as "privacy alarmists," while privacy is considered to be "old-fashioned", "overly expensive", and "a roadblock to innovation". This misconception has significant consequences for public policy and discourse and reinforces the legitimacy of the current flawed privacy rules that fail to safeguard people against unethical data practices.

Yelp, a popular review platform, boasts over 140 million local business reviews that aid customers in identifying local businesses. However, this abundance of information has other potential uses. For instance, Yelp reviews could help restaurants decide whether to add a bar or explore new markets. It can also assist property investors in identifying potential gentrification hotspots, or help private equity firms choose between Philz and Blue Bottle for investments in the coffee industry.

For managers making strategic data decisions, the vast data sets accumulated by private enterprises present both new opportunities and challenges. While there are numerous cases of data repurposing gone awry, it would be counterproductive for businesses to hoard their data. Instead, they should consider how their data can complement existing public data sources before dismissing its potential uses.

If personal information is not kept private or if individuals are unable to regulate how their information is used, it may be exploited in a variety of ways, including the following:

1) Discrimination and Evaluation: Personal information is used to assess indi-

viduals in accordance with predetermined standards or group them into entities for later treatment.

- *Identifying Political Opponents*
  Individuals can be identified as supporters of particular political movements, regimes, or candidates based on their publicly expressed beliefs and behaviour. For instance, a person's participation in a specific street protest can be inferred from their social media activities and smartphone location. In some nations, authorities combine vast amounts of data on individual citizens, including medical records, travel reservations, online purchases, social media comments, location data, and information on interpersonal relationships to identify people who are suspected of politically sensitive activity and act against the interests of the government. Private corporations from Western democracies have already provided assistance to authoritarian nations in finding and repressing their opponents. For example, Yahoo provided the email correspondence of two dissidents to a foreign government.
- *Unequal Hiring Procedures*
  A wide and growing range of personal data, including biometric information, health records, and social media data, is being used in recruitment decisions, leading to unfair and illegal employment practices. Companies specializing in employment screening provide employers with comprehensive background checks on specific prospective candidates.

2) Discrediting: Personal data is disclosed in ways that affect the data subject's legal status and/or reputation. The latter refers to the subject's regard and esteem held by friends, family, employers, colleagues, and other close social contacts in addition to the subject's status in society at large.
   - *Political Defamation Strategies*
     Negative information can be disseminated about an activist to damage their reputation, credibility, or political influence. This strategy is often used by businesses and public authorities to undermine their critics and opponents, in addition to election campaigns and dictatorial governments. Examples of such tactics include General Motors' actions against Ralph Nader, an advocate for automobile safety, the COINTELPRO scandal, in which US law enforcement agencies infiltrated and discredited civil rights and anti-war organizations, and the FBI's publication of Martin Luther King's extramarital affairs.
   - *Legal Evidence*
     Personal data collected by technological companies can be used to provide evidence of a person's unlawful behaviour to law enforcement officials or in court. Companies gather a wide variety of data about their customers, such as private emails, audio recordings captured by Amazon's Alexa, health and activity data from wearable fitness trackers, and comprehensive location records from Google Timeline. Law enforcement officials have previously requested such sensitive information as evidence. For example, Google received requests from authorities to hand over data from more than 340,000 user accounts in 2019 alone. While the production of evidence is vital to a functional legal system, excessive monitoring can undermine civil liberties. As Aleksandr Solzhenitsyn observed, "Everyone is guilty of something or has something to hide."

3) Personalized Persuasion: To boost a message's persuasive power, it is targeted and/or customized based on facts about the recipient (such as preferences, personality traits, political attitudes, and phobias).
   - *Commercial Advertising*
     The usage of personal data by social networking sites, search engines, and online ad networks to target specific audience members with advertisements is common. For example, "behavioural targeting" presents advertisements based on users' previous web usage and browsing habits. Empirical studies show that even targeting ads based on consumers' smallest signals of preference, such as a single Facebook "like," can have the psychological effect of persuading a large number of individuals. Advertisements can also be targeted based on a person's lifestyle, demographics (such as gender, age, income, and work status), current location, or even emotions and mental states, such as when they are depressed, afraid, or feel less beautiful. Additionally, algorithms are being developed to automatically replicate the visual characteristics of target individuals because consumers are more receptive to advertisements when they feature people who resemble them. These algorithms can be continuously refined and fine-tuned using data on people's attitudes and behaviour as real-time feedback until they achieve the desired manipulative effect.

4) *Accessing Protected Domains or Assets:* Personal information is used to access a data subject's private accounts, private property, or even the entire identity in order to access protected domains and assets of the subject.
   - *Identity Theft*
     Personal information, such as dates of birth, passport numbers, Social Security numbers, phone numbers, Medicare numbers, addresses, and financial account numbers, can be exploited by criminals for identity theft. With such information, criminals can impersonate individuals and carry out fraudulent activities, such as opening accounts, making purchases, or filing false tax returns in the victim's name. Despite being a long-standing problem, identity theft has become more prevalent in recent years. Criminals can access a victim's online accounts by using leaked passwords and answers to security questions, such as the victim's mother's maiden name. This can enable them to send messages and even threaten others on the victim's behalf. Identity theft victims often experience various negative consequences, including lawsuits, loan and government service denials, debt collection harassment, embarrassment, worry, and anxiety. Some emerging types of identity theft even use biometric samples to synthesize fingerprints or a victim's voice to deceive biometric authentication systems.

The misuse of private data in the political sector occurred during the 2014 US Presidential Elections when it was revealed that Donald Trump and his campaign had primarily focused on scraping, analyzing, and manipulating data from Facebook in order to secure the presidency. This illustrates the immense power that private data holds and how it can be abused to achieve different objectives, be it winning an election or gaining more views and consumers for a business.

Any of these outcomes can be detrimental to an individual. For a company, these consequences could result in penalties, sanctions, and other legal repercussions, in addition to causing irreparable harm to its reputation.

In addition to the practical implications of privacy infringements, many individuals and governments believe that privacy has intrinsic value as a human right essential to a democratic society, akin to the freedom of speech.

How Private Data Is the Biggest Business of this Century

Every day, billions of people use the internet, with Google alone receiving 8.5 million searches per day. While the daily services we use on our phones and laptops are free, we pay for them with our personal data. The process involves invading personal spaces to collect data and claiming ownership of that data for the corporation. Companies like Google have grown from profitable startups to multimillion-dollar enterprises in just a few years, thanks to the monetization of data.

The term "extraction architecture" refers to the interface between the physical and virtual worlds. In surveillance capitalism, the extraction process is almost entirely automated, benefiting the aforementioned firms and having little to no impact on consumers. Instead of being used to enhance the user experience, the data is sold to other businesses. Targeted advertisements aim to sell products, so the data is analyzed to predict behaviour and mould it accordingly. Personal data is then used to show users personalized ads or other similar experiences, feeding into a never-ending loop that has proven to be incredibly profitable.

However, the extraction architecture has several restrictions. Although the loop mentioned above is successful in producing additional raw material, quality must also be taken into account in order to more correctly forecast behaviour. The most accurate projections match observations, according to Zuboff. As a result, the type of data required must also broadly approximate observations. Economies of scope refer to this requirement for both a huge amount of high-quality data and a significant surplus of it. This comes into being in two steps:

1. Since the data gathered in the former must reflect the experiences had in the latter as precisely as possible, the data gathering must be expanded from the virtual world into the real world. As of now, online user inputs like likes and clicks have been the most popular ways to apply for this extension. The inference is that data collection efforts will also be made offline as a result of this. This would eliminate the requirement for the user to actively participate in data collection and instead rely on sensors or other devices that passively extract physical data.
2. This kind of extraction must obtain more detailed and private information about people. The economies of scope demand that user preference data not be restricted to the virtual environment because that is insufficient. The methods for gathering data are insufficient, so new approaches must be created and used in an effort to obtain even more sensitive and private information. Examples include facial recognition, affective computing, voice, gait, posture, and text analysis that reveal personality, moods, emotions, lies, and vulnerabilities.

As limitations are reached, stringent extraction escalation is mandated by the economies of scope. Economies of action, as Zuboff refers to them, enable this continuous escalation.

By definition, a Placebo is an artificial substance that doesn't deliver the stated benefit. However, the Placebo Effect is a very genuine phenomenon. Decades of research show that placebos (fake therapies) have produced genuine positive effects. When patients deliberately believe their treatment will be effective, the placebo effect manifests in very tangible ways. Also, receiving treatment—even with a "fake" drug—creates unconsciously positive connections that aid in recovery.

The Placebo Effect, which occurs when a person consumes a certain product and

is linked to data manipulation through the sale of data by huge organizations, can both be observed using the same phenomenon. To begin with, data brokers gather and extract information based on a person's preferences and needs, then sell it to companies so they can target and draw in consumers. A person would soon believe that the product or service targeted at them is a basic necessity in their lives due to the placebo effect if they are continually told how important it is for them to purchase or utilize a particular thing. This strategy allows firms to extend their customer base, which in turn increases the demand for data, making it one of the century's largest industries.

Role Of Artificial Intelligence

The goal of artificial intelligence (AI) is to create smart computers capable of performing tasks that traditionally require human intelligence. Machines equipped with AI can mimic or even surpass human brain functions. The development of AI is gradually integrating into everyday life, as demonstrated by the emergence of smart assistants such as Siri and Alexa, as well as the development of autonomous vehicles.

Artificially intelligent systems can perform actions frequently attributed to human cognitive abilities, such as understanding speech, playing games, and identifying patterns. They often acquire these skills by analyzing vast amounts of data and searching for patterns to mimic in their decision-making processes. Humans typically oversee the learning process of AI, rewarding intelligent decisions and critiquing poor ones.

Science fiction movies and books no longer exclusively feature AI technology. Our daily lives are quickly incorporating tech, thus we must adapt. Despite a general lack of familiarity, artificial intelligence is a technology that is revolutionizing all aspects of life. It is a versatile tool that helps individuals to reconsider how we combine information, evaluate data, and use the insights obtained to enhance decision-making. AI has the potential to alter and have an impact on our daily lives as it develops. It might accomplish this in a variety of ways, including the following:

1) *Home Automation*
   Home automation makes home security more intelligent. A home AI can be linked to linked IoT camera systems, alerting the user to any alterations in or around the home or any suspicious behaviour. If the AI notices something odd, camera systems can also be accessed from a phone or computer. Home security systems in general demand a lot of user involvement. A security system must be turned on or off from a nearby access point before leaving a house.
   This is no longer true thanks to AI-powered home automation. With just a voice command, security systems can be turned on or off. This enables remote access to a home security system via a computer or a mobile device.
2) *Smart Assistants*
   Almost all smartphones are outfitted with a virtual assistant that is specifically designed to meet the needs of the user. Examples of virtual assistant apps that come pre-installed on top smartphones include Apple's Siri, Samsung's Bixby, and Windows' Cortana. The significant time you save by letting the interface handle tasks for you is one of the more obvious benefits of virtual assistants. AI assistants can be programmed to update your customer records automatically, manage your to-do lists, and organize the copious quantities of emails you receive each day. Digital assistants can also help you become smarter over time. With a single order, you can access any fact or piece of knowledge you're interested in, but your VA may also give you puzzles, riddles, and other mental exercises. AI assistants also offer a lot more to ease our daily lives, such as reducing stress related to remembering simple chores you need to complete or even lightening your workload. AI assistants are useful for keeping track of your health, which has the potential to be very advantageous for the medical sector. Siri and Alexa are two excellent examples of AL Assistants that are incredibly beneficial and simplify one's life.
3) *In the Retail Sector*
   AI-based solutions are being used to revolutionize inventory management, offer individualized recommendations to improve customer experience, and increase supply chain management. Robots with AI capabilities are also being employed in warehouses to enhance order fulfilment and optimize inventory management. All of the recommendations you receive from e-commerce websites are generated by AI. AI assists in personalizing shopping experiences, making product recommendations, and forecasting consumer behaviour. To increase ROI, recommendation engines analyze consumer behaviour and forecast purchasing patterns. It optimizes inventory levels and supply chain management while automating pricing and replenishment processes.

There has been a recent increase in AI-led efforts because of the enormous promise that this technology provides for organizations. The most recent revolution—the ChatGPT—is one of these endeavours. Others include creating proactive customer services solutions like chatbots or predictive analytics for enhanced decision-making. Though being in its infancy and only known to be operating at 5-7% of its potential, today's AI still has significant limits. To more effectively direct resources and future research efforts, it is necessary to step back and honestly evaluate the merits and drawbacks of current AI. The next generation of AI needs to be more high-performing and resilient in order to demonstrate the great power that AI possesses, and in each of the areas covered below, promising work is already being done at the cutting edge of the field.

The development of Artificial Intelligence aims to create smart computers capable of performing tasks that traditionally require human intelligence. AI-equipped machines can mimic or even surpass human brain functions. The integration of AI into daily life is evidenced by the emergence of smart assistants like Siri and Alexa, as well as the development of autonomous vehicles.

However, the amazing ability of AI to mimic human intellect raises concerns that it may displace people. According to a recent assessment issued by the Organization for Economic Co-operation and Development (OECD) in March, 66 million jobs are highly automated, and 70% of jobs may be automated over the next 15 to 20 years. In an interview for CNBC, Jeff Bezos, the world's wealthiest man, expressed his optimism that AI will be beneficial and make humans happier, rather than taking away jobs.

AI can assist humans in various ways, including disaster relief efforts. However, poorly regulated algorithms and social media platforms can also be used for immoral and harmful purposes, as seen in Facebook's involvement in fake news and the 2016 elections. Huawei, a state-sponsored technology corporation in China, is considered a national security threat by the United States, Australia, New Zealand, Japan, Germany, and potentially Canada and the United Kingdom. The US government and other organizations also purchase services from Google and Microsoft. Elon Musk and Stephen Hawking have warned about the uncontrolled use of AI leading to catastrophe and crimes against humanity.

AI is learning more effective ways to communicate with and control people, as recent studies have shown that AI can recognize habits and behaviours that humans use to influence their decision-making. The problem is that AI systems can understand people even better than we understand ourselves because they can analyze vast amounts of data we leave behind in our digital trail. Every time we use Google to search, watch a movie online, visit a store, or post something on Instagram, we leave information about ourselves behind. Algorithms can understand our motives, interests, and even dislikes by identifying trends in this data.

Manipulation can occur when information is forced upon people without their consent or through skewed "news" or viewpoints that promote extremism, misinformation, and fearmongering. It is crucial that AI is used responsibly since it can be employed for good or bad. Last year, the Australian government developed an AI Ethics Framework as the first stage of this process. Since AI and machine learning are data-hungry, effective protocols for data governance and access must be established.

How Artificial Intelligence Can Be Used to Misuse Private Data of The Public

The first point to consider is that artificial intelligence operates at an incredibly rapid and efficient pace, despite not currently functioning at its full potential. To accumulate enough data, it is presently working at approximately 5-7% capacity, while still operating faster than the human brain. This capability is one of the factors that could make artificial intelligence an effective tool for misusing personal information obtained from individuals using the internet. As artificial intelligence continues to develop in the coming years, it may become capable of producing many quick results, which large enterprises and corporations may leverage to rapidly exploit data and influence the public. This could result in easier access to data for everyone, including major corporations seeking to promote their products, restaurants, businesses, and even political leaders.

The ethical implications of mishandling private data and utilizing it against people's wishes could potentially be minimized when artificial intelligence is involved in the manipulation and misuse of data. When AI is utilized, everything is treated more impartially since it is not programmed to discern differences in treatment and does not possess any emotions. This would improve the ethical and genuine nature of how AI uses data.

In terms of using AI as a tool to misuse public data, there would not be any human interaction involved since ethics are at stake whenever humans are involved. However, as previously mentioned, ethics would not be a valid consideration in this instance since there would not be any human intervention.

Compared to humans, artificial intelligence has several advantages and improvements when it comes to pattern recognition, optimization, speed, and effectiveness. When artificial intelligence gradually learns human patterns and behaviours to enhance its machine learning (ML) capabilities for data analysis and eventually manipulate and misuse private and public data, it will have untapped power that has not yet been fully realized.

How Can This Be Contained

Artificial intelligence will be operating at peak performance and will have the ability to instantly examine, tamper with, and alter data. In order to protect the data and limit the possible influence that AI could have over humans, measures

need also be taken against it.

First, one might begin by correctly optimizing AI to ensure that the data is secure and that no personal data is in danger. This could be accomplished by mandating that AI should not operate at a level beyond 70% so that it can function properly while not being so powerful as to negatively impact human existence.

The AI system might also be forced to have periodic human interaction with appropriate human morality and ethics in place. This will prevent AI from having any negative effects, and data can be collected fast and securely while remaining in the correct hands because AI cannot be used to misuse it.

To ensure that it is safe and cannot be further abused by the power of AI, the data that is left with it should never be particularly sensitive or of great value. If AI is going to be utilized to quickly extract, gather, and analyze data by creating patterns using its efficiency and ability, the governments might also be involved in order to legally set some laws in place.

All of these steps could be very helpful in completing the job with the proper attitude, proper ethics, and at the best and most efficient efficiency possible while employing artificial intelligence.

CONCLUSION

The vast amount of private information and data that these companies and organizations now hold will undoubtedly be exploited to either improve an individual's global experience or damage their reputation. The advent of Artificial Intelligence (AI) has increased the challenge even further. The global village's future will be shaped by AI in the ensuing decades and how it manages human digital footprints.

REFERENCES

1. "What Is Data Privacy? | Privacy Definition." Cloudflare, 2023, www.cloudflare.com/learning/privacy/what-is-data-privacy/. Accessed 20 Mar. 2023.
2. Jani, James. "Data Brokers: The Dark Industry of Selling Your Identity for Profit." YouTube, YouTube Video, 16 Mar. 2020, www.youtube.com/watch?v=uZ2l-kk5ihk. Accessed 20 Mar. 2023.
3. Ellis, Matt. "How to Write a Research Paper: A Step-By-Step Guide | Grammarly Blog." How to Write a Research Paper: A Step-By-Step Guide | Grammarly Blog, Grammarly Blog, 3 Feb. 2022, www.grammarly.com/blog/how-to-write-a-research-paper/. Accessed 20 Mar. 2023.
4. SANS. "Privacy vs. Security: It's a Log Story - sans CTI 2019 Keynote." YouTube, YouTube Video, 30 May 2019, www.youtube.com/watch?v=Jo0mbomZuhQ. Accessed 20 Mar. 2023.
5. "Research or Academic Studies Come in Different Forms. But Whether They Are Research Projects, Essays for Coursework, or Scientific Papers for Publication, They All Have One Thing in Common. And That Is a Thesis Statement. The Thesis Statement Is Made up of One or Two Sentences That Concisely Summarize the Main Points..." Research.com, Research.com, 3 May 2022, research.com/research/how-to-write-a-thesis-statement. Accessed 20 Mar. 2023.
6. "What Is Privacy Worth? | the Journal of Legal Studies: Vol 42, No 2." The Journal of Legal Studies, 2013, www.journals.uchicago.edu/doi/abs/10.1086/671754. Accessed 20 Mar. 2023.
7. . "Data Privacy Explained | Cybersecurity Insights #11." YouTube, YouTube Video, 12 Feb. 2019, www.youtube.com/watch?v=3YIPQrEWOeY. Accessed 20 Mar. 2023.
8. Winegar, A. G., and C. R. Sunstein. "How Much Is Data Privacy Worth? A Preliminary Investigation." Journal of Consumer Policy, vol. 42, no. 3, July 2019, pp. 425–40, https://doi.org/10.1007/s10603-019-09419-y. Accessed 20 Mar. 2023.
9. Short, James, and Steve Todd. SPRING 2017 ISSUE What's Your Data Worth? no. 3, www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/short-whats-your-data-worth.pdf.
10. "What Are the Most Common Breaches of the Right to Personal Data Protection (Personal Data Misuse)? - Gov.hr." Gov.hr, gov.hr/en/what-are-the-most-common-breaches-of-the-right-to-personal-data-protection-personal-data-misuse/1882.
11. Kröger, Jacob Leon, et al. "How Data Can Be Used against People: A Classification of Personal Data Misuses." SSRN Electronic Journal, 2021, https://doi.org/10.2139/ssrn.3887097. Accessed 20 Mar. 2023.
12. Esguerra, Richard. "Google CEO Eric Schmidt Dismisses the Importance of Privacy." Electronic Frontier Foundation, 11 Dec. 2009, www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy. Accessed 20 Mar. 2023.
13. Street, Farnam. "Why Privacy Matters Even If You Have 'Nothing to Hide.'" Farnam Street, 19 Dec. 2012, fs.blog/why-privacy-matters-even-if-you-have-nothing-to-hide/. Accessed 20 Mar. 2023.
14. Solove, Daniel. "10 Reasons Why Privacy Matters - TeachPrivacy." TeachPrivacy, 20 Jan. 2014, teachprivacy.com/10-reasons-privacy-matters/. Accessed 20 Mar. 2023.
15. Cohen, Julie. WHAT PRIVACY IS FOR. harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf.
16. Hull, Gordon. "Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data." Ethics and Information Technology, vol. 17, no. 2, May 2015, pp. 89–101, https://doi.org/10.1007/s10676-015-9363-z. Accessed 20 Mar. 2023.
17. Jacob Leon Kröger, et al. "The Myth of Individual Control: Mapping the Limitations of Privacy Self-Management." SSRN Electronic Journal, 2021, www.semanticscholar.org/paper/The-myth-of-individual-control%3A-Mapping-the-of-Kr%C3%B6ger-Lutz/ddd0506800eee025ae30a23fec66bf516d4c09bf. Accessed 20 Mar. 2023.
18. "How Do App Vendors Respond to Subject Access Requests? A Longitudinal Privacy Study on IOS and Android Apps | Proceedings of the 15th International Conference on Availability, Reliability and Security." ACM Other Conferences, 2020, dl.acm.org/doi/10.1145/3407023.3407057. Accessed 20 Mar. 2023.
19. "The Age of Surveillance Capitalism." Profile Books, profilebooks.com/work/the-age-of-surveillance-capitalism/.
20. Microsoft 365. "How to Write an Introduction for a Research Paper." Microsoft 365, 10 Aug. 2021, www.microsoft.com/en-us/microsoft-365-life-hacks/writing/how-to-write-an-introduction-for-a-research-paper. Accessed 20 Mar. 2023.
21. News, DW. "Who's Winning the Legal Battle against Big Data and Disinformation | Business Beyond." YouTube, YouTube Video, 3 Mar. 2023, www.youtube.com/watch?v=OfNjRj4wWAg. Accessed 20 Mar. 2023.
22. "The Power of the Placebo Effect - Harvard Health." Harvard Health, Harvard Health, May 2017, www.health.harvard.edu/mental-health/the-power-of-the-placebo-effect. Accessed 20 Mar. 2023.
23. "Surveillance Capitalism: An Essay - Free Essay Example - Edubirdie." Edubirdie, 2022, edubirdie.com/examples/surveillance-capitalism-an-essay/. Accessed 20 Mar. 2023.
24. Liu, Wendy, et al. "Placebo Effects of Marketing Actions: Consumers May Get What They Pay For." ACR European Advances, vol. E-07, 2019, www.acrwebsite.org/volumes/13843/eacr/vol7/E-07. Accessed 20 Mar. 2023.
25. "Why All Great Marketing Contains the Power of the Placebo Effect - Copyblogger." Copyblogger, 11 Feb. 2019, copyblogger.com/placebo-effect-marketing/. Accessed 20 Mar. 2023.
26. "G.M. Settles Nader Suit on Privacy for $425,000 (Published 1970)." The New York Times, 2023, www.nytimes.com/1970/08/14/archives/gm-settles-nader-suit-on-privacy-for-425000-gm-pays-nader-425000-in.html. Accessed 20 Mar. 2023.
27. Wikipedia Contributors. "COINTELPRO." Wikipedia, Wikimedia Foundation, 16 Mar. 2023, en.wikipedia.org/wiki/COINTELPRO. Accessed 20 Mar. 2023.
28. "You May Have 'Nothing to Hide' but You Still Have Something to Fear | ACLU." American Civil Liberties Union, 2 Aug. 2013, www.aclu.org/news/national-security/you-may-have-nothing-hide-you-still-have-something-fear. Accessed 20 Mar. 2023.
29. Solove, Daniel J. "A Taxonomy of Privacy." Penn Carey Law: Legal Scholarship Repository, 2014, scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/. Accessed 20 Mar. 2023.
30. Rosen, Rebecca J. "How Your Private Emails Can Be Used against You in Court." The Atlantic, theatlantic, 8 July 2011, www.theatlantic.com/technology/archive/2011/07/how-your-private-emails-can-be-used-against-you-in-court/241505/. Accessed 20 Mar. 2023.
31. "IF THESE WALLS COULD TALK: THE SMART HOME and the FOURTH AMENDMENT LIMITS of the THIRD PARTY DOCTRINE on JSTOR." Jstor.org, 2017, www.jstor.org/stable/44865635. Accessed 20 Mar. 2023.
32. Jacob Leon Kröger, et al. "How Data Can Be Used against People: A Classification of Personal Data Misuses." ResearchGate, unknown, 30 Dec. 2021, www.researchgate.net/publication/357431331_How_Data_Can_Be_Used_Against_People_A_Classification_of_Personal_Data_Misuses. Accessed 20 Mar. 2023.
33. Wikipedia Contributors. "Cancer Ward." Wikipedia, Wikimedia Foundation, 11 Feb. 2023, en.wikipedia.org/wiki/Cancer_Ward. Accessed 20 Mar. 2023.
34. "Google Transparency Report." Google.com, 2023, transparencyreport.google.com/user-data/overview?hl=en. Accessed 20 Mar. 2023.
35. Christl, Wolfie, and Sarah Spiekermann. Networks of Control. 2016, crackedlabs.org/en/networksofcontrol. Accessed 20 Mar. 2023.
36. Greenemeier, Larry. "What Is the Big Secret Surrounding Stingray Surveillance?" Scientific American, 25 June 2015, www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/. Accessed 20 Mar. 2023.
37. Cooke, Kristina. "U.S. Police Used Facebook, Twitter Data to Track Protesters - ACLU." U.S., 11 Oct. 2016, www.reuters.com/article/social-media-data-idINL4N1CH4J1. Accessed 20 Mar. 2023.
38. Cooke, Kristina. "U.S. Police Used Facebook, Twitter Data to Track Protesters - ACLU." U.S., 11 Oct. 2016, www.reuters.com/article/social-media-data-idINL4N1CH4J1. Accessed 20 Mar. 2023.
39. Verhulst, Stefaan. "China Seeks Glimpse of Citizens' Future with Crime-Predicting AI." The Living Library, 24 July 2017, thelivinglib.org/china-seeks-glimpse-of-citizens-future-with-crime-predicting-ai/. Accessed 20 Mar. 2023.
40. Wang, Amy B. "A Suspect Tried to Blend in with 60,000 Concertgoers. China's Facial-Recognition Cameras Caught Him." Washington Post, The Washington Post, 13 Apr. 2018, www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/. Accessed 20 Mar. 2023.
41. Schneier, Bruce, and Alicia Wanless. "Persuasion Is Essential to Society and Democracy, but We Need New Rules Governing How Big Tech Companies Can Harness It." Foreign Policy, Foreign Policy, 11 Dec. 2020, foreignpolicy.com/2020/12/11/big-tech-data-personal-information-persuasion/. Accessed 20 Mar. 2023.
42. Wikipedia Contributors. "Targeted Advertising." Wikipedia, Wikimedia Foundation, 31 Jan. 2023, en.wikipedia.org/wiki/Targeted_advertising. Accessed 20 Mar. 2023.
43. MacAskill, Ewen. "Yahoo Forced to Apologise to Chinese Dissidents over Crackdown on Journalists." The Guardian, The Guardian, 14 Nov. 2007, www.theguardian.com/technology/2007/nov/14/news.yahoo. Accessed 20 Mar. 2023.
44. Lutz, Otto Hans-Martin, et al. "Surfing in Sound: Sonification of Hidden Web Tracking." Gatech.edu, Georgia Institute of Technology, 2019, http://hdl.handle.net/1853/61533. Accessed 20 Mar. 2023.
45. "How Much Can Behavioral Targeting Help Online Advertising? | Proceedings of the 18th International Conference on World Wide Web." ACM Conferences, 2023, dl.acm.org/doi/10.1145/1526709.1526745. Accessed 20 Mar. 2023.
46. Raschke, Philip, et al. "Towards Real-Time Web Tracking Detection with T.EX - the Transparency EXtension." ResearchGate, unknown, 8 June 2019, www.researchgate.net/publication/334745947_Towards_Real-Time_Web_Tracking_Detection_with_TEX_-_The_Transparency_EXtension. Accessed 20 Mar. 2023.
47. Tiffany, Kaitlyn. "Online Ads Can Be Targeted Based on Your Emotions." Vox, Vox, 21 May 2019, www.vox.com/the-goods/2019/5/21/18634323/new-york-times-emotion-based-ad-targeting-sadness. Accessed 20 Mar. 2023.
48. Matz, S. C., et al. "Psychological Targeting as an Effective Approach to Digital Mass Persuasion." Proceedings of the National Academy of Sciences, vol. 114, no. 48, Nov. 2017, pp. 12714–19, https://doi.org/10.1073/pnas.1710966114. Accessed 20 Mar. 2023.
49. Moses, Lucia. "Marketers Should Take Note of When Women Feel Least Attractive." Adweek.com, Adweek, 2 Oct. 2013, www.adweek.com/brand-marketing/marketers-should-take-note-when-women-feel-least-attractive-152753/. Accessed 20 Mar. 2023.
50. Swathi Meenakshi Sadagopan. "Feedback Loops and Echo Chambers: How Algorithms Amplify Viewpoints." The Conversation, 4 Feb. 2019,

theconversation.com/feedback-loops-and-echo-chambers-how-algorithms-amplify-viewpoints-107935. Accessed 20 Mar. 2023.
51. "Identity Theft: An Overview of the Problem." The Justice Professional, 2023, www.tandfonline.com/doi/abs/10.1080/0888431022000070458. Accessed 20 Mar. 2023.
52. Anderson, Keith B., et al. "Identity Theft." Journal of Economic Perspectives, vol. 22, no. 2, Mar. 2008, pp. 171–92, https://doi.org/10.1257/jep.22.2.171. Accessed 20 Mar. 2023.
53. Skiba, Katherine. "Pandemic Proves to Be Fertile Ground for Identity Thieves." AARP, AARP, 5 Feb. 2021, www.aarp.org/money/scams-fraud/info-2021/ftc-fraud-report-identity-theft-pandemic.html. Accessed 20 Mar. 2023.
54. Armerding, Taylor. "Thieves Can Steal Your Voice for Authenticatoin." CSO Online, 16 May 2017, www.csoonline.com/article/3196820/vocal-theft-on-the-horizon.html. Accessed 20 Mar. 2023.
55. Burns, Ed, et al. "What Is Artificial Intelligence (AI)?" Enterprise AI, TechTarget, 2023, www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence. Accessed 20 Mar. 2023.
56. "What Is Artificial Intelligence (AI)? How Does AI Work? | Built In." Builtin.com, 2021, builtin.com/artificial-intelligence. Accessed 20 Mar. 2023.
57. West, Darrell M., and John R. Allen. "How Artificial Intelligence Is Transforming the World." Brookings, Brookings, 24 Apr. 2018, www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/. Accessed 20 Mar. 2023.
58. "Smart Home Technology: Making Life Easier with Automation." Devmio - Software Know-How, 2022, devm.io/iot/smart-home-ai-iot-160479-001. Accessed 20 Mar. 2023.
59. Guest Blog. "How Can AI Assistants Make Your Life Easier?" RE•WORK Blog - AI & Deep Learning News, RE•WORK Blog - AI & Deep Learning News, 16 Aug. 2019, blog.re-work.co/how-can-ai-assistants-make-your-life-easier/. Accessed 20 Mar. 2023.
60. Yarlagadda, Ravi Teja. "Future of Robots, AI and Automation in the United States." Ssrn.com, 8 Feb. 2015, papers.ssrn.com/sol3/papers.cfm?abstract_id=3803010. Accessed 20 Mar. 2023.
61. Arora, Sumit. "Power of Artificial Intelligence | Machine Learning Internship | Career Launcher." Machine Learning Internship, 2016, www.careerlauncher.com/machine-learning/internship/machine-learning-the-power-of-artificial-intelligence.html. Accessed 20 Mar. 2023.
62. ET Online. "How Artificial Intelligence Is Changing Your Life Unknowingly." The Economic Times, Economic Times, 15 Mar. 2023, economictimes.indiatimes.com/news/how-to/how-artificial-intelligence-is-changing-your-life-unknowingly/articleshow/98455922.cms. Accessed 20 Mar. 2023.
63. "You Are Being Redirected..." Analyticsinsight.net, 2023, www.analyticsinsight.net/power-of-artificial-intelligence-how-it-can-be-used-to-manipulate-people/. Accessed 20 Mar. 2023.
64. Toews, Rob. "What Artificial Intelligence Still Can't Do." Forbes, 9 Nov. 2022, www.forbes.com/sites/robtoews/2021/06/01/what-artificial-intelligence-still-cant-do/?sh=68577d8066f6. Accessed 20 Mar. 2023.
65. admin-ectnews. "AI Is Still in Its Formative Years." E-Commerce Times, 4 May 2017, www.ecommercetimes.com/story/ai-is-still-in-its-formative-years-84505.html. Accessed 20 Mar. 2023.
66. "Smartphone Statistics 2023: How Many People Have Smartphones?" EarthWeb, 9 Mar. 2023, earthweb.com/smartphone-statistics/. Accessed 20 Mar. 2023.
67. Bureau, ET. "4G Device Base Crosses 607 Million Mark in 2020; 5G Units at 2 Million: Report." The Economic Times, Economic Times, 11 Feb. 2021, economictimes.indiatimes.com/industry/telecom/telecom-news/4g-device-base-crosses-607m-mark-in-2020-5g-units-at-2-m/articleshow/80868957.cms. Accessed 20 Mar. 2023.
68. Ringel, Gal. "Council Post: Why Data Privacy Is Good for Business: Online Privacy as a Branding Imperative." Forbes, 21 Apr. 2022, www.forbes.com/sites/forbestechcouncil/2021/10/07/why-data-privacy-is-good-for-business-online-privacy-as-a-branding-imperative/?sh=676981c4297e. Accessed 20 Mar. 2023.
69. Simmons, Dan. "17 Countries with GDPR-like Data Privacy Laws." Comforte.com, 2022, insights.comforte.com/countries-with-gdpr-like-data-privacy-laws. Accessed 20 Mar. 2023.
70. Romm, Tony. "Governments in 30 Countries Manipulated Media Online to Silence Critics, Sow Unrest or Influence Elections." Vox, Vox, 14 Nov. 2017, www.vox.com/2017/11/14/16640300/internet-freedom-facebook-twitter -google-us-russia-disinformation. Accessed 20 Mar. 2023.
71. "Data Privacy Laws by Country 2023." Worldpopulationreview.com, 2023, worldpopulationreview.com/country-rankings/data-privacy-laws-by-country. Accessed 20 Mar. 2023.
72. "Your Personal Data and How Companies Use It." Cbscreening.co.uk, 2017, cbscreening.co.uk/news/post/your-personal-data-and-how-companies-use-it/. Accessed 20 Mar. 2023.
73. "How Trump Consultants Exploited the Facebook Data of Millions (Published 2018)." The New York Times, 2023, www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Accessed 20 Mar. 2023.
74. "How Donald Trump Campaign Used Data Scraped from Facebook to Win Presidency." The Independent, 23 Mar. 2018, www.independent.co.uk/news/world/americas/facebook-scandal-latest-donald-trump-campaign-presidential-election-cambridge-analytica-steve-bannon-a8269706.html. Accessed 20 Mar. 2023.
75. "How Companies Can Use the Data They Collect to Further the Public Good." Harvard Business Review, 16 May 2018, hbr.org/2018/05/how-companies-can-use-the-data-they-collect-to-further-the-public-good. Accessed 20 Mar. 2023.
76. "AI and Privacy: Everything You Need to Know." Ericsson.com, 2022, www.ericsson.com/en/blog/2022/8/ai-and-privacy-everything-you-need-to-know. Accessed 20 Mar. 2023.
77. "Artificial Intelligence (AI) – What It Is and Why It Matters." Sas.com, 2022, www.sas.com/en_in/insights/analytics/what-is-artificial-intelligence.html. Accessed 20 Mar. 2023.
78. "What Is AI Analytics?" Anodot, 24 May 2022, www.anodot.com/learning-center/ai-analytics/. Accessed 20 Mar. 2023.
79. Sham, Swaroop. "What Is Data Misuse?" Okta.com, Okta Inc., 10 Mar. 2022, www.okta.com/blog/2020/06/data-misuse/. Accessed 20 Mar. 2023.